

SAML: What's Next?

Dr. Carlisle Adams

Principal Architect – Advanced Security

Senior Cryptographer

Entrust, Inc.

Outline

- Background
- SAML v1.1
- SAML v2.0
- Some specific examples
- Proposed timeline

Background

- SAML v1.0
 - Published November 5, 2002, after roughly
 - 19 months of TC activity, and
 - 3 months of OASIS approval process
 - From multiple initial proposals to approved standard in less than 2 years is remarkable
 - Achievable only if
 - Some features left “out of scope”
 - Some errors slip through ☺

Background (cont'd)

- Two alternatives
 1. Publish errata document; Quit.
 2. Work on subsequent versions of SAML
- Security Services TC chose option “2”
 - v1.1: errata & backward compatible changes
 - v2.0: new features, richer functionality

SAML v1.1

- List of work items
 - Errata (section #s, formatting, font, spelling, etc.)
 - Versioning clarification (assertions & protocols)
 - Guidelines for use of XML Signature with SAML
 - Addition of DoNotCache condition
 - Specification of metadata for interoperability
 - Web browser profile for “Destination Site First”
 - Switch to absolute URIs; deprecation of fragmentID
 - Deprecation of RespondWith and AuthorityKind
 - Use of base64 in form post, UTF-8 in SourceLocation

SAML v2.0

- List of potential work items
 - Session management (e.g., coordinated logout)
 - Liberty requirements (richer SSO, metadata, NameId exchange, etc.)
 - Assertion confidentiality (using XML Encryption)
 - Profiles for multi-participant transactional workflows
 - Binding for HTTP
 - Privacy and anonymity features (e.g., anonymous name identifier)
 - Kerberos support
 - Use of intermediaries
 - More complex queries (e.g., “all attributes in namespace X”)
 - Credentials Collector model and protocols
 - Alignment of AuthorizationDecisionQuery/Response with XACML

SAML v2.0 (cont'd)

- Several other items on “potential” list as well
 - see SS TC mail list archives:
<http://lists.oasis-open.org/archives/security-services/200302/msg00053.html>

Outline

- Background
- SAML v1.1
- SAML v2.0
- Some specific examples
- Proposed timeline

Credentials Collector

- Purpose
 - Simplify the task of the Authentication Authority
- Method
 - Translate proprietary formats for credentials or message protocols into standard formats, **OR**
 - Perform authentication of the user locally and simply request that the AA issue the assertion
- Technology
 - Make use of WS-Trust specification, SASL framework, or some other mechanism (still under discussion)

AuthDecisionQuery/Rep

- Revision of current ADQ/ADR
 - Generalization to accommodate the possibility of multiple subjects, hierarchical resources, and the return of obligations for the PEP to fulfill
 - Needed to satisfy use cases encountered in XACML (specifically in the protection of health records, J2SE objects, and Web resources)
 - Current ADQ/ADR will be deprecated in favour of this revision

Outline

- Background
- SAML v1.1
- SAML v2.0
- Some specific examples
- Proposed timeline

Proposed Timeline

- SAML 1.1
 - Committee Specification: end of May, 2003
 - OASIS Open Standard: end of August, 2003
- SAML 2.0
 - Committee Specification: end of year, 2003
 - OASIS Open Standard: early 2004